Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 620926, 8 pages
http://dx.doi.org/10.1155/2014/620926

Research Article

A New Mechanism for Network Monitoring and Shielding in Wireless LAN

Jiujun Cheng,[1,2] Liufei Hu,[2] Junjun Liu,[2] Qingyang Zhang,[2] and Chendan Yan[2]

[1] *Department of Computer Science and Technology, Tongji University, Shanghai 201804, China*
[2] *Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji University, Shanghai 201804, China*

Correspondence should be addressed to Liufei Hu; huliufei2008@126.com

Received 5 December 2013; Accepted 21 January 2014; Published 10 March 2014

Academic Editor: Huaicheng Yan

Wireless LAN (WLAN) technology is developing rapidly with the help of wireless communication technology and social demand. During the development of WLAN, the security is more and more important, and wireless monitoring and shielding are of prime importance for network security. In this paper, we have explored various security issues of IEEE 802.11 based wireless network and analyzed numerous problems in implementing the wireless monitoring and shielding system. We identify the challenges which monitoring and shielding system needs to be aware of, and then provide a feasible mechanism to avoid those challenges. We implemented an actual wireless LAN monitoring and shielding system on Maemo operating system to monitor wireless network data stream efficiently and solve the security problems of mobile users. More importantly, the system analyzes wireless network protocols efficiently and flexibly, reveals rich information of the IEEE 802.11 protocol such as traffic distribution and different IP connections, and graphically displays later. Moreover, the system running results show that the system has the capability to work stably, and accurately and analyze the wireless protocols efficiently.

1. Introduction

The IEEE 802.11 wireless LAN standard was established in 1989 and was originally intended to seek a wireless equivalent to Ethernet [1]. Since then, wireless technology has been grown tremendously with flexibility. WLAN is a computer local area network using wireless channel as transmission medium and is a combinative product of computer and wireless communication technology. WLAN uses the public electromagnetic waves as a carrier to transmit data signals; thus one of the major issues which needs to be addressed is security. WLAN security technology research has also been rapidly developed with the development and application of wireless LAN.

Many security issues in the IEEE 802.11 WLAN have been identified and demonstrated in many studies [1–7]. The study of Boland and Mousavi [1] in Proceedings of the Canadian Conference on Electrical and Computer Engineering was one of the earlier studies. They introduced the importance of security and proposed several security issues in WLAN. WLAN security system consists of three different components: authentication, encryption, and WLAN. The issues in encryptions [5] and authentication [6] mechanisms have been demonstrated. In paper [3], they identified and demonstrated two MAC vulnerabilities, identity vulnerability and media access vulnerability. These flaws indicate that wireless shielding technology and protocol analysis are very important for effective network diagnosis.

As wireless LAN technology has many irreplaceable advantages, and its development is very rapid. In recent years, WLAN has been widely used in the family, school, or some places that are not suitable for wiring or enterprises and occasions that need mobile office environment. But it also brings some new attendant issues, such as security issues for wireless networks and management oversight. Many studies [7–13] on measurement and characterization of wireless LANs and wireless monitoring have been performed. The authors in [8] addressed two problems: wireless monitoring technique and its applications in MAC traffic characterization and network diagnosis. They first identified the pitfalls of wireless monitoring and provided two feasible solutions, namely, merging multiple sniffers and their placement. Then, they applied those techniques to academic research WLAN over two weeks for MAC traffic characterization and network diagnosis.

Wireless monitoring is of prime importance for WLAN security. More importantly, wireless monitoring exposes the characteristics on the wireless network itself so that we can infer more information. Such wireless monitoring allows us to know physical layer header information including signal strength, noise level, and data rate for individual packets. Similarly, it also enables examination of the link layer headers, which include IEEE 802.11 type and control fields. The information can be used to examine network problems and throughput. By analyzing the MAC layer data, we can characterize traffic according to different frame types, namely, data, control, and management frames. The collected data, combined with timestamps, can be used as accurate traces of the IEEE 802.11 link-level operations. Such traces are useful when we want to emulate the protocol or diagnose the problems of wireless networks [8].

In more general wireless environment, in paper [10], a novel 4G multiplatform real-time monitoring system is presented giving emphasis to WLAN part. The main idea of this system is to collect reports from numerous network elements in such way that the system is compatible and operational in any kind of network of any manufacturer and operator. Additionally the system architecture discussed in the paper is capable of accommodating and supporting 4G networks effectively.

In this paper, we focus on proposing a useful mechanism for wireless monitoring and shielding technique based on all the above advantages, implementing an effective wireless monitoring and shielding system, and showing its effectiveness in security monitoring, data sniffer, and protocol analysis. The remainder of this paper is organized as follows. Section 2 presents the proposed wireless monitoring and shielding mechanism and the implement of system. Section 3 shows and discusses the experimental results. Finally, we conclude our works in Section 4.

2. Wireless LAN Monitoring and Shielding Mechanism

Wireless monitoring is an effective mean to understand network performance and behavioral characteristics and improve network efficiency. According to whether inserting probings traffic into network, there are two kinds of wireless monitoring technologies, active monitoring and passive monitoring. To capture the detailed information, wireless monitoring technique can be used.

In this paper we have proposed a new mechanism for wireless LAN monitoring and shielding. Figure 1 illustrates wireless LAN monitoring environment, AP represents wireless access point, and wireless devices mainly include mobile phone and computer.

Figure 2 shows the process of our mechanism for wireless monitoring and shielding. It is user-centered and demonstrates the operating mechanism in detail. The mechanism involves five parts: User, User Interface, Data Buffer, Protocol Analysis, and Network, which will be introduced in detail in the following section. We give a brief introduction for mechanism process as follows.

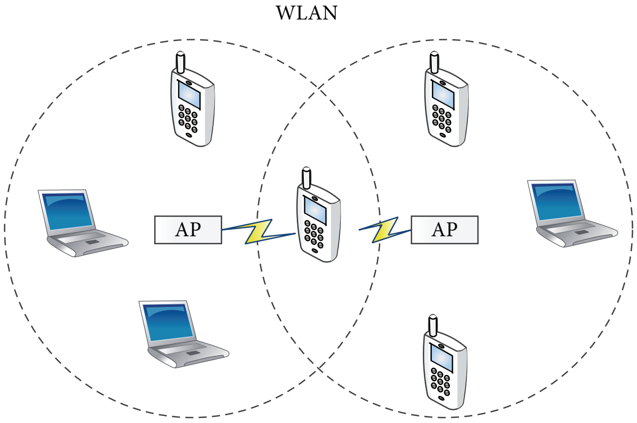


Figure 1: Wireless monitoring environment.

(1) First, the User Interface Module emits a signal to Data Buffer Module every second when no operation happened. Then the Data Buffer Module updates the signal and emits the updated signal to the User Interface Module. Finally, the User Interface Module transforms the data into graphical data and shows them to users (*steps 1–3*).

(2) In case that the user does not have some operation, whenever it captures a new data packet from network card, the following two tasks will be done. First, the Network Module will send the data packet to the Protocol Analysis Module. Then, the Protocol Analysis Module processes the data and stores the data structure into Data Buffer Module (*steps 4–6*).

(3) When the user executes an operation or sends a request, the User Interface Module will send a message to the Data Buffer Module to obtain the information; after receiving the message, the Data Buffer Module will start to collect on-demand information and return these information to the User Interface Module; the User Interface Module will transfer the data into graphical data and display them to the user (*steps 7–10*).

(4) The User Interface Module sends a command signal to Protocol Analysis Module; the Protocol Analysis Module will change analyzing methods based on the received information and process network data packet in different way. At the same time, the Protocol Analysis Module will send a signal to the Data Buffer Module and require it to change its storage format according to the user request. At last, the User Interface Module will update the information which is displayed and provide user with the needed information (*steps 11–15*).

Based on the above mechanism, we implemented a network monitoring and shielding system, which is running

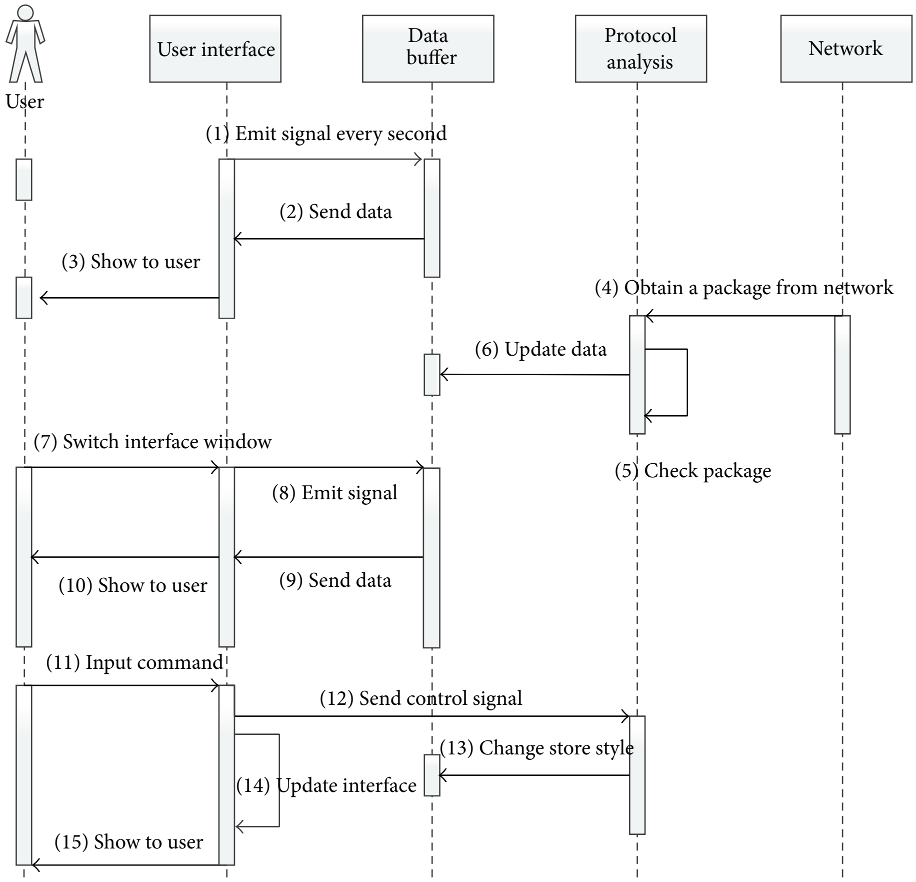


Figure 2: Process of mechanism.

on Maemo operating system, a software platform developed by Nokia and then handed over to Hildon Foundation for smartphones and Internet tablets [14] and is named Maemo Shield.

2.1. Maemo Shield Architecture. Maemo Shield is a lightweight network monitoring and shielding system which is run on the mobile and portable devices. To some extent, it can solve the security problems for mobile users. Figure 3 shows the system architecture which consists of Colleting Network Data, System Management, User Interface, and the most import Protocol Analysis Module and so on.

The first step is to collect all the needed data from network stream for the monitoring process. The wireless monitoring system consists of a set of devices which we call sniffers [12, 13], to capture network packets and observe traffic characteristics on the wireless medium. This step collects raw data directly from NIC driver layer taking advantage of sniffer technology, namely, network data capture. We retain whole packets information from raw data, which is the most complete network stream.

After the data collection, the system starts to perform the Protocol Analysis Module, which is the most critical and difficult module. The data packets obtained by previous step will be transferred into Protocol Analysis Module. In this module, all packets headers will be analyzed.

The result of protocol analysis will be stored in the Data Buffer Pool for the use of the latter part and these data will be from the buffer pool after finish the work in protocol analysis procedure. And the released space will be used to store other network data. In order to make these intermediate results be fully utilized, we use the Analyze and Calculate Module to do the secondary analysis and processing.

At this time, the System Management Module is used to coordinate the operating parameters of various analyses and save some configuration. In order to improve the operational efficiency, Maemo Shield uses multithread technology to implement network date capture and protocol analysis. Therefore, it requires a global management module to control the exclusive and parallel processes among threads.

The last but not least is the User Interface. It is the operational interface between system and users. After processing data in detail, the results will be showed to users in the way of diversified image which includes information in text form, in list form, in histogram form, in pie chart form, in grid form, and so on. The system will present dynamic graphical information which is transformed from data by the User Interface to users. At the same time, the User Interface sends the users requests to the management system and these requests will directly responded by the Protocol Analysis Module through processing the captured network data.

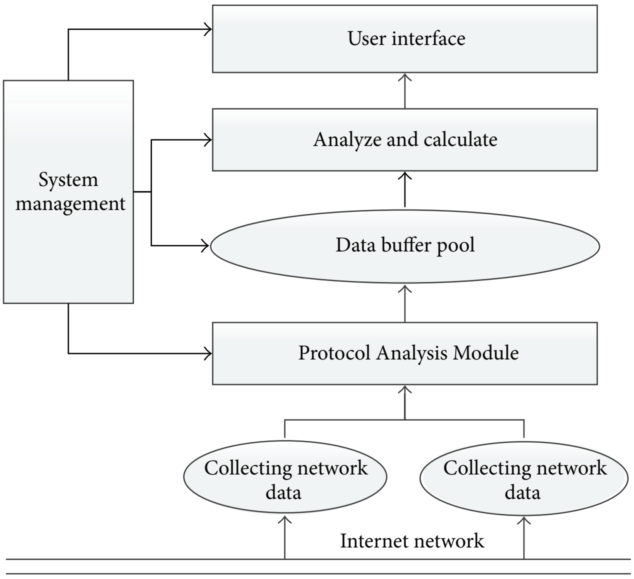


Figure 3: System architecture.

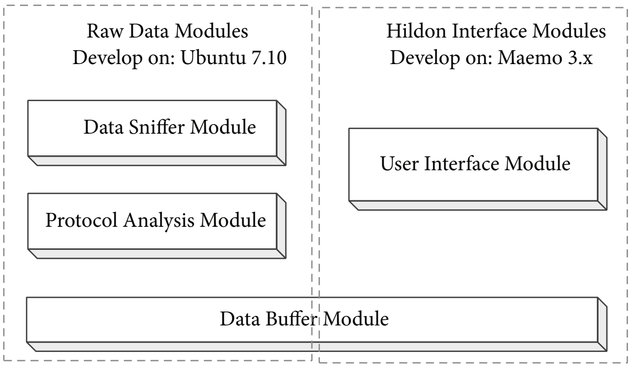


Figure 4: System modules.

2.2. The System Modules. Since the operation of the system involves both the network data capturing and the displaying of the high-level Hildon framework, so we will divide the development process of the system into two parts like Figure 4, which demonstrates the system modules, which includes Data Sniffer Module, Protocol Analysis Module, and User Interface Module and gives emphasis to Protocol Analysis Module.

The function of Raw Data Modules is to analyze and control the underlying network data. The system is running on the Nokia's N770/N800/N810 Internet Tablets series. Because the running speed of these devices is relatively slow, if the achievement and analysis of network data of system are developed on these devices directly then the efficiency of the development will be lower and the complexity of system debugging will be higher. Therefore we will extract the common part between those devices and Linux development platform. And we will use the efficient development tools to develop and debug in Linux platform. Then we will modify these modules slightly and inject them into the development system of Nokia.

The function of Hildon Interface Modules is to provide users efficient and dynamic graphics on the Nokia's Maemo development platform. This part will take full advantage of the unique realistic characteristics of Maemo. And all special good features which are not compatible with Linux will be achieved in this part.

(1) *Data Sniffer Module* obtains full data flow information from NIC directly, which will contain all the data stream packet header and message body.

(2) *Protocol Analysis Module* analyzes obtained data following different protocols from data linker layer, network layer, transport layer, and application layer. Analysis information will be stored in the data buffer module for secondary analysis and display.

(3) *Data Buffer Module* is an independent part of the system by constructing and procedures abstract data storage structure to preserve the structure of protocol analysis and to complete the information and data share.

(4) *User Interface Module* uses GTK +2.0 and Hildon GUI technology to present information in data buffer pool for user, and the user can operate the system with this module.

2.3. Protocol Analysis. Wireless monitoring is widely used in both wireless LAN and wireless LAN security management research. Moreover, wireless monitoring mechanism is also adopted in wireless protocol analysis. Wireless protocol information is very important for security monitoring in the IEEE 802.11 wireless LAN. It is well known that the IEEE 802.11 WLAN has security vulnerability due to the flaws in the MAC protocol [3] and basic features of wireless networks, such as open medium and mobility. To correctly diagnose such security problems we need to monitor wireless network

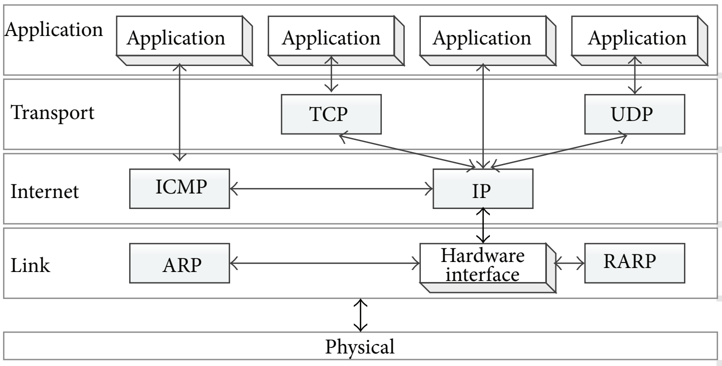


Figure 5: TCP/IP protocol stack.

information instantaneously. Therefore, such instantaneous wireless information, security monitoring, and surveillance are very important for effective network security.

The protocol stack used in this system is based on TCP/IP [15, 16] instead of the 7-layer OSI reference model; TCP/IP protocol stack are communication protocols using four-layer structure, each layer invoking network services provided by the next layer to meet their needs (Figure 5). These four layers are as follows.

(i) *Application layer* is an interapplication communication layer, such as Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Network Remote Access Protocol (Telnet).

(ii) *Transport layer* provides data transmission services among nodes, such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Its main function is to format data and provide a mechanism for the transmission of data.

(iii) *Network layer* provides the basic transmission function of data packet and guarantees that packets reach the destination hosts but does not check if received correctly, such as Internet Protocol (IP).

(iv) *Link layer* manages the actual network media, defines how to use the Internet to transmit data, and is responsible for receiving the network layer datagram and sending through the transmission line.

The transmitted data should be encapsulated through protocol by the system. The first step is to use application layer protocol to encapsulate data, such as HTTP. HTTP protocol is based on TCP protocol. It is encapsulated by the TCP and HTTP as data part of TCP data segment. The TCP protocol is based on the IP protocol. So the TCP segment can be regarded as the payload and added with IP header to be an IP datagram. The IP datagram is Ethernet-based, so this time it is encapsulated into an Ethernet frame, and then the system sends the data by Ethernet frames. After receiving network data, the system will be the decomposer of data packets. Decompose process and encapsulate process on the contrary.

The total process of protocol analysis (Figure 6) begins with the data link layer to analyze and decompose packets, via the network layer to the transport layer, and ends with the final analysis of application layer.

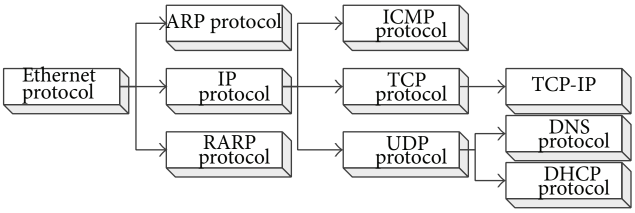


Figure 6: Process of protocol analysis.

After obtaining WLAN network source data, first of all, we analyze those data and parse management frame, data frame, and control frame, respectively. Then use statistical data to understand network data composition and structure. In order to implement WLAN protocol analysis, firstly, we should know structure, composition, and topology of wireless LAN; what is more, we must be familiar with the structure of a radio frame, namely, MAC frame format to analyze, and statistic detailed information from frame; in addition, we also need to understand TCP/IP protocol stack to analyze upper level data from the network layer and transport layer; finally, we use these statistics to analyze network data composition and draw and display information.

Protocol Analysis Module is mainly based on the MAC frame format. It respectively parses bits of every field in MAC frame corresponded to every field, respectively, to comprehend the structure of each frame as well as its details and significance. Wireless LAN MAC frame has three kinds of frames, data, control, and management frame. Management frame is used for connection and separation to the site with the access point, timing, synchronization, and authentication; control frame is used for handshake communication and positive confirmation during competition period and ends in noncompetition period; data frame is used for transmitting data between competition period and noncompetition period and combined with acknowledgment (ACK) frame together in the noncompetition period. Therefore, we must distinguish these types of frames before separating and parsing each frame, respectively. After distinguished frame type of each frame, the next step is to handle three types of frames separately.

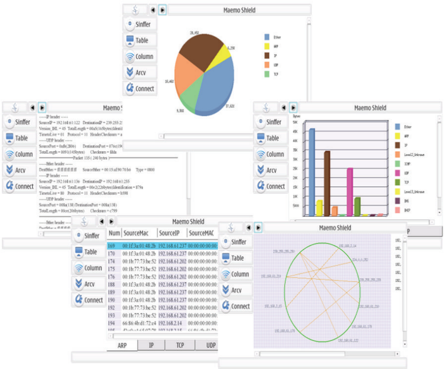


Figure 7: Protocol analysis view.

After the original data was processed and analyzed in accordance with the specific protocol format, User Interface Module gets data from the processed packet buffer and graphically displays the statistic information about packets. See Figure 7, and the details are displayed in Section 3.

3. Analysis of Experimental Results

In this section, we will present our experimental results. The purpose of those experiments is to analyze the wireless monitoring technique in terms of its effectiveness in capturing wireless packets and to present precise statistics information. We set up our device using the Maemo operating system with kernel version 4.1 to capture 802.11 frame information including the IEEE 802.11 header as well as physical layer header and information of higher layer protocols. In the rest of this section we will show the results of our experiment.

3.1. Capture and Analyze Packet Based on Sniffer. The system intercepts every packet through NIC and analyzes bit stream of the data packet. Then it will show the packet information of link layer, network layer, and transport layer in a recognizable manner to the screen in real time.

For example, we will analyze the 135th packet in Figure 8.

=======Packet 135 (240 bytes)========

It indicates that the packet is the 135th packet and length is 240 bytes.

- - - - Ether header - - - - - -

Dest Ether = ff:ff:ff:ff:ff:ff

Source Ether = 00:15:af:90:70:b6

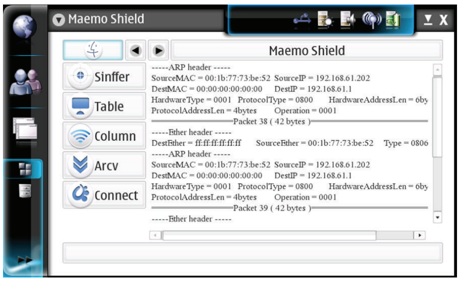
Type = 0800

It shows that Ethernet protocol is used in link layer, source Mac address is 00:15:af: 90 : 70:b6, and destination Mac address is ff:ff:ff:ff:ff:ff. The protocol identification of upper layer is 0800.

- - - - - IP header - - - - - -

Source IP = 192.168.61.136

Destination IP = 192.168.61.255



```
-----ARP header -----
SourceMAC = 00:1b:77:73:be:52  SourceIP = 192.168.61.202
DestMAC = 00:00:00:00:00:00    DestIP = 192.168.61.1
HardwareType = 0001  ProtocolType = 0800    HardwareAddressLen = 6by
ProtocolAddressLen = 4bytes      Operation = 0001
─────────────────Packet 38 ( 42 bytes )─────────────────
-----Ether header -----
DestEther = ff:ff:ff:ff:ff:ff     SourceEther = 00:1b:77:73:be:52    Type = 0806
-----ARP header -----
SourceMAC = 00:1b:77:73:be:52  SourceIP = 192.168.61.202
DestMAC = 00:00:00:00:00:00    DestIP = 192.168.61.1
HardwareType = 0001  ProtocolType = 0800    HardwareAddressLen = 6by
ProtocolAddressLen = 4bytes      Operation = 0001
─────────────────Packet 39 ( 42 bytes )─────────────────
-----Ether header -----
```

Figure 8: Capture and analyze packet.

Version_IHL = 45

Total Length = 00e2 (226 bytes)

Identification = 879a

Time to LIve = 80

Protocol = 11

Header Checksum = b698

It shows that the network layer using IP protocol source address is 192.168.61.136, and destination address is 192.168.61.255. After removing link layer header, the length of packet is 226 bytes. Network identification number is 879, and the protocol identification of upper layer is 11. Survival time is 80; header checksum is b798.

- - - - - UDP header - - - - -

Source Port = 008a (138)

Destination Port = 008a (138)

Total Length = 00ce (206 bytes)

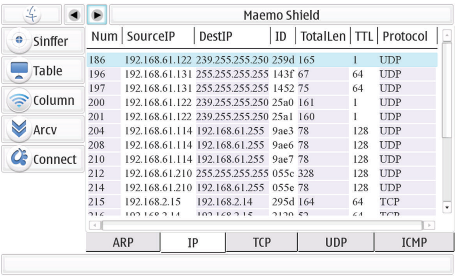
Checksum = c799

It says that transport layer uses the UDP protocol, source port is 138, and destination port is 138. After removing linker layer and network layer header, the length of packet is 206 bytes, and packet checksum is c799.

We can get complete information of packet from the data link layer to the network layer through these series data.

3.2. Analysis of Protocol. The system records the recent 20 data records which use ARP, IP, TCP, UDP, and ICMP protocols and displays the protocol header information in list form. Maemo Shield has a buffer buffering the data packet protocol header information of five different protocols, so we can select the switches lower side of the table function panel to view different protocol header information. See Figure 9.

3.3. Protocol and IP Oriented Analysis of Network Stream. The system analyzes network stream by protocol oriented and IP oriented analysis and displays the data in the form of a histogram. In actual operation, the histogram is in the form of dynamic growth from the bottom up, and the whole process is done automatically. Figure 10 demonstrates that Ether protocol datagrams are used at most, followed by the IP datagram should be noted that Level2_Unknown and Level3_Unknown mean, respectively, the system does not



Num	SourceIP	DestIP	ID	TotalLen	TTL	Protocol
186	192.168.61.122	239.255.255.250	259d	165	1	UDP
196	192.168.61.131	255.255.255.255	143f	67	64	UDP
197	192.168.61.131	255.255.255.255	1452	75	64	UDP
200	192.168.61.122	239.255.255.250	25a0	161	1	UDP
201	192.168.61.122	239.255.255.250	25a1	160	1	UDP
204	192.168.61.114	192.168.61.255	9ae3	78	128	UDP
208	192.168.61.114	192.168.61.255	9ae6	78	128	UDP
210	192.168.61.114	192.168.61.255	9ae7	78	128	UDP
212	192.168.61.210	255.255.255.255	055c	328	128	UDP
214	192.168.61.210	192.168.61.255	055e	78	128	UDP
215	192.168.2.15	192.168.2.14	295d	164	64	TCP

Figure 9: Analysis of protocol.

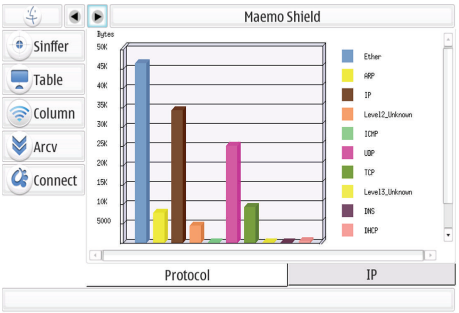


Figure 10: Protocol oriented analysis of network stream.

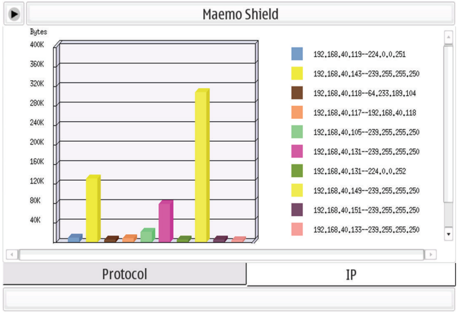


Figure 11: IP oriented analysis of network stream.

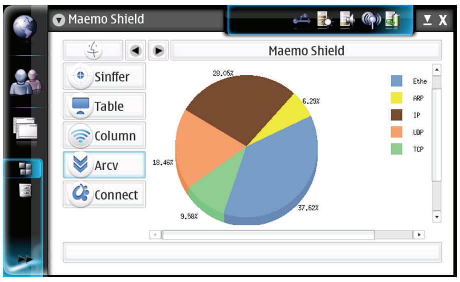


Figure 12: Stream distribution based on protocols.

recognize datagram protocol of the network layer and the transport layer. In Figure 11, 192.168.40.148-239.255.255.250 traffic ratio is the highest one among all connections, and 192.168.40.117-192.168.40.118 is the second highest share of traffic. It has four IP connections, whose traffic is relatively stable, while other connection data traffic is relatively small. We can determine that the initial connection to other noise may be invalid connections, while four high-traffic connections are the focus of our attention; they directly related to the process devices.

3.4. Stream Distribution Based on Protocols. Network data stream is divided under the protocols and displayed in pie graph. In the graph, different colors represent different protocols, the larger area occupied sector corresponds to the greater traffic of the protocol, and the percent indicated at its edges represents the percentage in the data stream protocol traffic ratio. In Figure 12, it shows the relative distribution of the data stream protocol: ether share 37.62%, ARP representing 6.29%, IP accounting for 28.05%, UDP accounting for 18.46%, and TCP accounted for 9.58%.

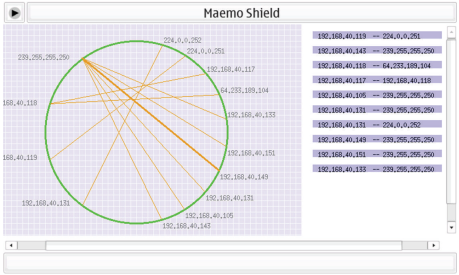
It should be noted that the data represented by these protocols at different levels may be double counted, the share traffic ratio is not a fixed value. For example, 6.29% of ARP and IP is included in the 37.62% of ether. Because ARP and IP protocol used by the data link layer protocols is ether, so their traffic is less than Ether protocol traffic certainly. Similarly, TCP and UDP traffic share values must also be included in the value of IP traffic.

3.5. Connections Related to Device. The system expressed IP connections associated with the device IP connection in the form of mesh. In Figure 13, it shows that there are 10 IP connections connected to the device in the left panel, and there is a thick orange line in 10 connections, which indicates that the traffic of the current connection is the largest one. The right panel shows these connections clearly and the data transfer volume.

The system running results demonstrate the effectiveness of the mechanism in capturing the packets, presenting statistics, and analyzing protocols. The proposed mechanism has been implemented in the mobile devices. Real packet monitoring has been done and results have been recorded. So the system has the capability to work stably and accurately and analyze the wireless protocols efficiently.

4. Conclusion

In this paper we have researched various issues about wireless security and analyzed numerous problems in implementing the WLAN. We implemented an actual wireless LAN monitoring system to monitor the network data transmission, allowing users to understand the situation of device. What is more, the system analyzes and records ARP, RARP, IP, UDP, TCP, ICMP, and other protocols efficiently and flexibly. In the same time, statistics network data stream allows users to understand the data transmission protocol and type, as well as their share of the network bandwidth, respectively. Moreover, the system monitoring the IP connections allows users to know data communications of connected devices and identify the one communicating with device most frequently. Finally, the system can save the network traffic logs in debug mode. The results show that the system has the capability to work stably and accurately and analyze the wireless protocols efficiently.



```
192.168.40.119  -- 224.0.0.251
192.168.40.143  -- 239.255.255.250
192.168.40.118  -- 64.233.189.104
192.168.40.117  -- 192.168.40.118
192.168.40.105  -- 239.255.255.250
192.168.40.131  -- 239.255.255.250
192.168.40.131  -- 224.0.0.252
192.168.40.149  -- 239.255.255.250
192.168.40.151  -- 239.255.255.250
192.168.40.133  -- 239.255.255.250
```

Figure 13: Connections related to device.

It is not easy to analyze some wireless network information such as the network running status and operating efficiency because of some features of IEEE 802.11 WLAN. It is now being developed and there are many problems which are worth of in-depth study and research. In this system, besides protocol information, other information can be obtained. We can provide more information of the traffic characteristics and connection status of WLAN. The research needs to propose new and more effective ways to handle those issues.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by Natural Science Foundation Programs of Shanghai Grant no. 13ZR1443100, by ISTCP under Grant 2013DFM10100, by the National Science and Technology Support Plan Grant no. 2012BAH15F03, and by NSFC under Grants 51174210, 61003102, and 61103072.

References

[1] H. Boland and H. Mousavi, “Security issues of the IEEE 802.11B wireless LAN,” in *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, vol. 1, pp. 0333–0336, May 2004.

[2] IEEE Computer Society LAN MAN Standards Committee, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 1997.

[3] J. Bellardo and S. Savage, “802.11 Denial-of-service Attacks: real vulnerabilities and practical solutions,” in *Proceedings of the USENIX Security Symposium*, pp. 15–28, 2003.

[4] H. Zhang, H. Yan, F. Yang, and Q. Chen, “Quantized control design for impulsive fuzzy networked systems,” *IEEE Transactions on Fuzzy Systems*, vol. 19, no. 6, pp. 1153–1162, 2011.

[5] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in *Selected Areas in Cryptography*, pp. 1–24, Springer, Berlin, Germany, 2001.

[6] B. C. Neuman and T. Ts’o, “Kerberos. An authentication service for computer networks,” *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[7] A. Mishra and W. A. Arbaugh, “An initial security analysis of the IEEE 802.1 X standard,” 2002.

[8] H. Yan, H. Shi, H. Zhang, and F. Yang, “Quantized H_∞ control for networked systems with communication constraints,” *Asian Journal of Control*, vol. 15, no. 5, pp. 1468–1476, 2013.

[9] J. Yeo, M. Youssef, and A. Agrawala, “A framework for wireless LAN monitoring and its applications,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe ’04)*, pp. 70–79, October 2004.

[10] D. Nikitopoulos, A. Trakos, I. Popescu, and K. Xenou, “Real-time WLAN monitoring in a 4G multiplatform environment,” in *Proceedings of the IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC ’06)*, pp. 1–5, September 2006.

[11] K. Thompson, G. J. Miller, and R. Wilder, “Wide-area internet traffic patterns and characteristics,” *IEEE Network*, vol. 11, no. 6, pp. 10–23, 1997.

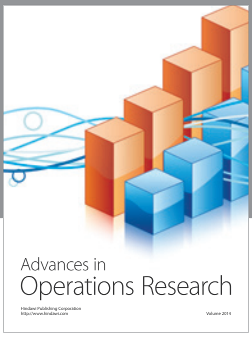
[12] A. Dabir and A. Matrawy, “Bottleneck analysis of traffic monitoring using wireshark,” in *Proceedings of the 4th International Conference on Innovations in Information Technology (IIT ’07)*, pp. 158–162, November 2007.

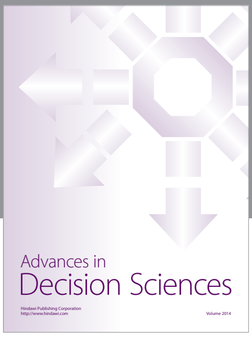
[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. Siddiqui, “Network traffic analysis and intrusion detection using packet sniffer,” in *Proceedings of the 2nd International Conference on Communication Software and Networks (ICCSN ’10)*, pp. 313–317, February 2010.

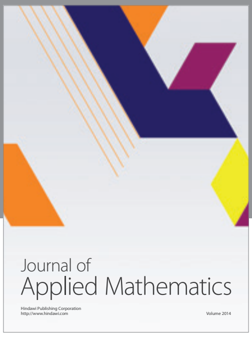
[14] S. Ansari, S. G. Rajeev, and H. S. Chandrashekar, “Packet sniffing: a brief introduction,” *IEEE Potentials*, vol. 21, no. 5, pp. 17–19, 2002.

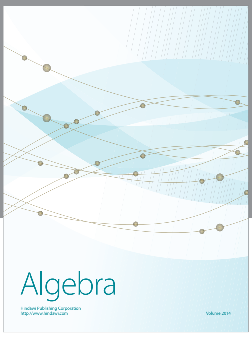
[15] N. Ahmed, N. Ahmed, and A. Q. K. Rajput, “TCP/IP protocol stack analysis using MENeT,” in *Proceedings of the IEEE Conference on Convergent Technologies for the Asia-Pacific Region (TENCON ’03)*, vol. 4, pp. 1329–1333, October 2003.

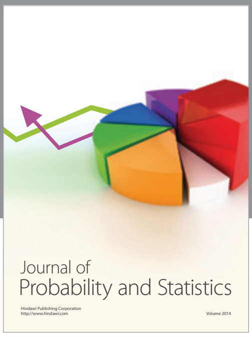
[16] N. A. Junejo, N. Ahmed, and A. Q. K. Rajput, “Network layer packet analysis using MENeT,” in *Proceedings of the 7th International IEEE Multi Topic Conference (INMIC ’03)*, pp. 151–156, 2003.


Advances in
Operations Research

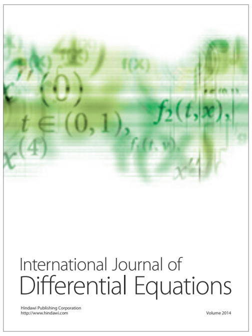

Advances in
Decision Sciences


Journal of
Applied Mathematics

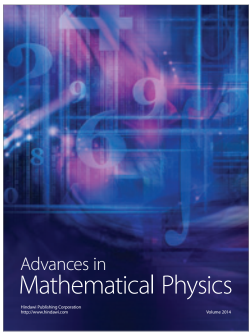

Algebra

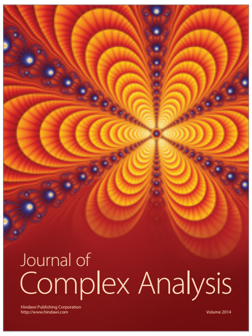

Journal of
Probability and Statistics

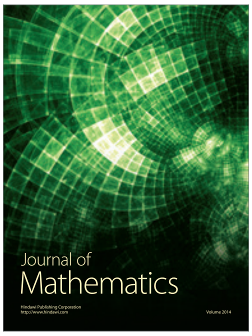
The Scientific
World Journal

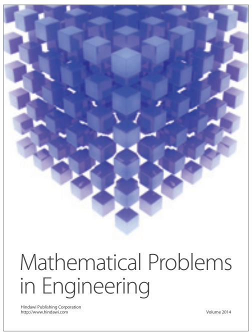

International Journal of
Differential Equations

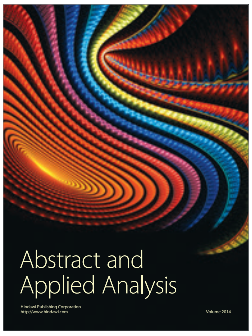
International Journal of
Combinatorics

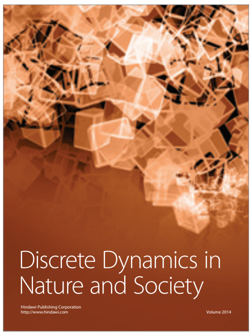

Advances in
Mathematical Physics

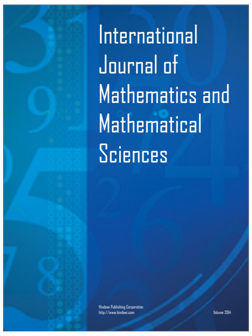

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

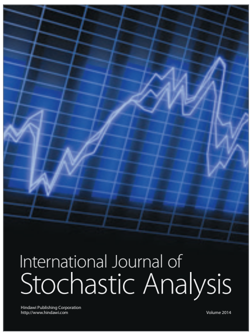

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization